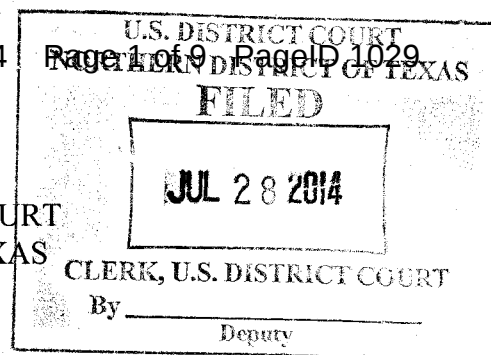


ORIGINAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

UNITED STATES OF AMERICA

v.

CHRISTOPHER ROBERT WEAST

§
§
§
§
§

4:14-CR-0023 - A

DEFENDANT CHRISTOPHER ROBERT WEAST'S
BRIEF IN SUPPORT OF THE ADMISSIBILITY OF THE TESTIMONY OF
BILL MCGERGOR.

COMES NOW, the Defendant, CHRISTOPHER ROBERT WEAST, by his counsel, Christopher A. Curtis, Assistant Federal Public Defender, and hereby files this brief in support of the admissibility of the testimony of Bill McGregor, in the above styled case, and shows the Court the following:

I.

On July 18, 2014, the defendant filed a motion to supplement its notice of expert by naming Bill McGregor as an expert. The defendant has disclosed to the Court and the government that the defense would like to present the testimony of Mr. McGregor on two primary points: 1) computers are susceptible to remote access and hacking; and (2) it is impossible to look at a visual image and know if it depicts an actual minor. On July 25, 2014 the Court held a hearing, pursuant to *Daubert v. Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579, 592-93 (1993), to determine the admissibility of McGregor's testimony. At the conclusion of the hearing, the Court granted the defendant leave to designate McGregor as an expert and asked the parties to submit briefs by 8:30 a.m. July 28, 2014, the morning of trial, regarding the admissibility of McGregor's testimony.

II.

The defense first is addressing the anticipated testimony of McGregor concerning his ability to testify that computers in general, as well as the computer in question, are susceptible to hacking or remote access via the internet, via wireless routers, via access by other individuals, and via other means. During the hearing on July 25, 2014, McGregor testified to this factor as is expected he will testify to when called as a witness by the defense. (See Transcript of July 25, 2014 Hearing, pp. 10-11).

For the information of the Court, at the conclusion of the hearing on Friday, July 25, 2014 the attorney for the government Aisha Saleem informed the attorneys for the defense that she was not opposed to McGregor's testimony as it was presented during the July 25 hearing. Also, on Sunday, July 27, 2014, undersigned counsel conferred again with Ms. Saleem and she confirmed that she was not opposed to that testimony.

For further information of the Court, Mr. McGregor did personally meet with the government's expert Jim Willingham on the afternoon of July 25, 2014, and reviewed the virus scans conducted by the government's forensic expert and discussed in the July 25 hearing. Mr. McGregor confirmed his opinion that the computer in question is susceptible to remote access or hacking. Mr. Willingham also confirmed this fact.

Accordingly, it does not appear that there is any dispute concerning Mr. McGregor's testimony in this regard. Moreover, the defense, after reviewing the transcript of Mr. McGregor's testimony contends that his testimony meets the standards of *Daubert*. Evidence that the computer in question could have been remotely accessed is highly relevant to the element of whether the defendant downloaded the images in question and whether he knowingly possessed the images.

Mr. McGregor is clearly qualified to testify to the fact that computers in general, as well as the computer in question, are susceptible to remote access and hacking.

III.

The government also objected to McGregor's testimony that no-one can possibly tell from viewing an image downloaded off the internet whether that image is an image of an actual person. McGregor is an expert who lists as a key competency "Forensically image storage on digital devices including computers, mobile devices and video devices." The defendant's expert has a B.S. Degree in Internet System Software Technology, is completing his Masters in Management Information Systems (MSMIS)/ Minor in Digital Forensics, has an associates degree in Information Systems Technology, and several other qualifications. The defendant has worked for the government on computer systems with Top Secret Clearances. The defendant has specifically prepared reports in child pornography cases on the very issue that is being addressed in this case. (See Transcript of July 25, 2014 Hearing, p. 24). The defendant specifically explained the method used to determine whether a digitally stored image has been altered or manipulated, that is, by looking at the meta data and EXIF data for the image, and made it clear that this is one of his areas of expertise. (See Transcript of July 24, 2014 Hearing, pp. 11-17). McGregor also testified clearly and definitively that regarding images stored digitally on a computer, there is simply no way to tell if the images are of real minors, or if they have been manipulated or not manipulated. (See *id.*). McGregor made it clear that this honest and simple fact that the defense intends to present to the jury is common knowledge within the IT community. (See Transcript of July 24, 2014, Hearing, pp. 16-17). This simple fact also seems to be accepted by Congress, the government's own experts, and the courts.

For example, the very same legislation the government is relying on to prosecute the defendant was based upon findings that are precisely what the defendant seeks to prove to the jury in this case. In fact, findings were made in 1995 when Congress enacted the law that attempted to allow the government to prosecute images that were not of actual minors. The United States Congress, in passing the "A Child Pornography Prevention Act of 1995," made the following findings:

Congress finds:

...

(5) new photographic and computer imaging technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from unretouched photographic images of actual children engaging in sexually explicit conduct;

(6) computers and computer imaging technology can be used to-

(A) alter sexually explicit photographs, films, and videos in such a way as to make it virtually impossible for unsuspecting viewers to identify individuals, or to determine if the offending material was produced using children;

(B) produce visual depictions of child sexual activity designed to satisfy the preferences of individual child molesters, pedophiles, and pornography collectors; and

(C) alter innocent pictures of children to create visual depictions of those children engaging in sexual conduct;

Child Pornography Prevention Act of 1995, SENATE REPORT NO. 104-358, '2 (August 27, 1996);

see also id. at *7, Part I, *8, part III., '2, & **15-20, Part IV(b).

And further, as the defense has already argued in a previous filing, in 2001, the Fifth Circuit pointed out that the government's own expert has admitted the very fact that the government now seeks to prevent the defendant from presenting to the jury:

Perhaps most importantly, Congress has advanced a powerful new rationale for the necessity of the "appears to be" language in § 2252A: the need to address the law enforcement problem created by tremendous advances in computer technology . . . ,

advances that have greatly exacerbated the already difficult prosecutorial burden of proving that an image is of a real child. n33 Without the “appears to be” language in the statute, “there is frequently a built-in reasonable-doubt argument as to the age of the participant, unless the government can identify the actual child involved.” n34 During the trial in the instant case, for example, **Special Agent Barkhausen, the government’s computer expert, was forced to concede under cross-examination that “there’s no way of actually knowing that the individual depicted [in the images] . . . even exists[.]”** The “appears to be” language, then, is necessary to confront the enforcement problems that have been increased by these advancements in computer technology.

United States v. Fox, 248 F.3d 394, 403 (5th Cir. 2001).

Moreover, the Department of Justice itself, has made the very same argument to the Supreme Court that the defense wishes to present to the jury in this case. In *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 254-255 (2002), where the government was trying to save the law that allowed for prosecution of images that were not of real minors, the Supreme Court noted:

Finally, the Government says that the possibility of producing images by using computer imaging makes it very difficult for it to prosecute those who produce pornography by using real children. Experts, we are told, may have difficulty in saying whether the pictures were made by using real children or by using computer imaging. The necessary solution, the argument runs, is to prohibit both kinds of images. The argument, in essence, is that protected speech may be banned as a means to ban unprotected speech. This analysis turns the First Amendment upside down.

There simply is no question or dispute that technology exists where what appears to be child pornography can be created from an otherwise completely innocent image of a child. See *Doe v. Boland*, 630 F.3d 491, 493 (6th Cir. 2011) (Where a defense expert was actual prosecuted and sued for creating what appeared to be child pornography from an innocent picture in order to show how no-one could ever possibly tell with absolute certainty whether an image is that of a

real minor).

The Federal Rules of Evidence allows opinion testimony, from an expert witness that is qualified as an expert by knowledge, skill, experience, training, or education, if the such testimony will assist the trier of fact in making a valid jury determination. The other prerequisites for opinion testimony to be granted consist of: (1) The testimony is based on sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the expert has reliably applied the principles and methods to the facts of the case. *FED. R. EVID.* 702. The supreme court ruled that it is the responsibility of the trial courts to determine if expert testimony is not only relevant, but reliable. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

In the present case, there simply is no dispute that the sought after testimony is based upon sufficient facts and data. The images being prosecuted are digital images being stored on a computer. McGregor has been provided the meta data and EXIF data connected to those images. McGregor has extensive knowledge, education and expertise concerning the storage of digital images and is an expert in that field. He has relied on proper principles and methods as is evidenced by the fact that Congress, the Supreme Court, Court of Appeals for the Fifth Circuit, and the government itself have recognized repeatedly the very principle McGregor is expected to testify to in this case. McGregor has applied that principle reliably as is evidenced by the fact that his opinion is entirely consistent with the authority above. It is only the government's opposition to this testimony that is inconsistent with the above-cited authority.

The government seems to be taking the position that this testimony is not admissible because the defense should be presenting some evidence from a photoshop expert or a graphic

design expert. This position is absurd and completely ignores the entire point, not only of the testimony sought after by the defense, but also the point the government has taken until the trial of this case. The point is that if the image alleged in the indictment is a digital image from a computer – no-one can tell from looking at that image whether it is an image of a real minor. If the defense were to bring a photoshop expert into court – if there is such an expert – the government would likely object to that expert as being unqualified to testify to the point being made by the defense. The only reason you would bring an authenticating witness to authenticate whether an image is unaltered would be if you had an original image to compare to the digital image, which we do not have in this case. (See Transcript of the July 25 2014 Hearing, p. 22).

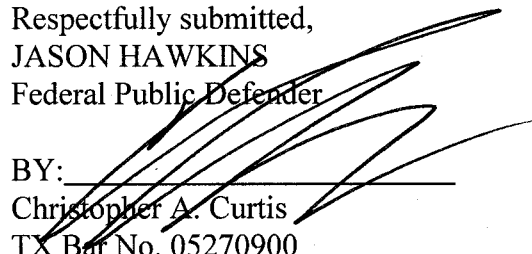
The government's attempt to bring in a law enforcement officer to testify he has seen the digital image and also has met the person alleged to be in the image (five years after the image was allegedly created) also completely ignores the fatal flaw in the government's case. Whether the witness Wine knows the alleged victim in this case, whether the witness Wine can testify that he recognizes the victim in the digital image, still does not prove that the image the government is trying to prosecute is an image of a real child. The problem is this is a digitally stored image. No-one can possibly tell the jury this image is that of an actual child except for possibly the person in the image and possibly the person who created the image. The government has chosen to allege that the images in this case are those of a real minor. The government has chosen not to bring the only reliable proof to the jury of this fact, that is, the testimony of the alleged minor, or the testimony of the person who created these images.

Failure to allow the defendant the opportunity to present the apparently undisputable fact that when it comes to a digitally stored image, no-one can tell the jury with absolute certainty that

the image is of a real or actual minor will deprive the defendant's constitutional right to a trial by jury on all the elements of the offense, to call witnesses on his own behalf, and to confront witnesses against him, as guaranteed by the Sixth Amendment, as well as his due process rights under the Fifth Amendment.

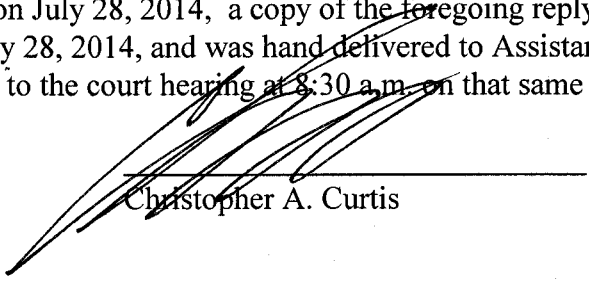
Wherefore, the defendant prays the Court find the testimony of Bill McGregor to be admissible in the trial of this case.

Respectfully submitted,
JASON HAWKINS
Federal Public Defender

BY: 
Christopher A. Curtis
TX Bar No. 05270900
Asst. Federal Public Defender
819 Taylor Street, Room 9A10
Fort Worth, TX 76102-6114
817-978-2753
Attorney for Defendant

CERTIFICATE OF SERVICE

I, Angela Saad, hereby certify that on July 28, 2014, a copy of the foregoing reply was e-mailed to Aisha Saleem the morning of July 28, 2014, and was hand delivered to Assistant United States Attorney Aisha Saleem prior to the court hearing at 8:30 a.m. on that same date.



Christopher A. Curtis